2002

The Great Cyberwar of 2002

Arquilla, John

WIRED

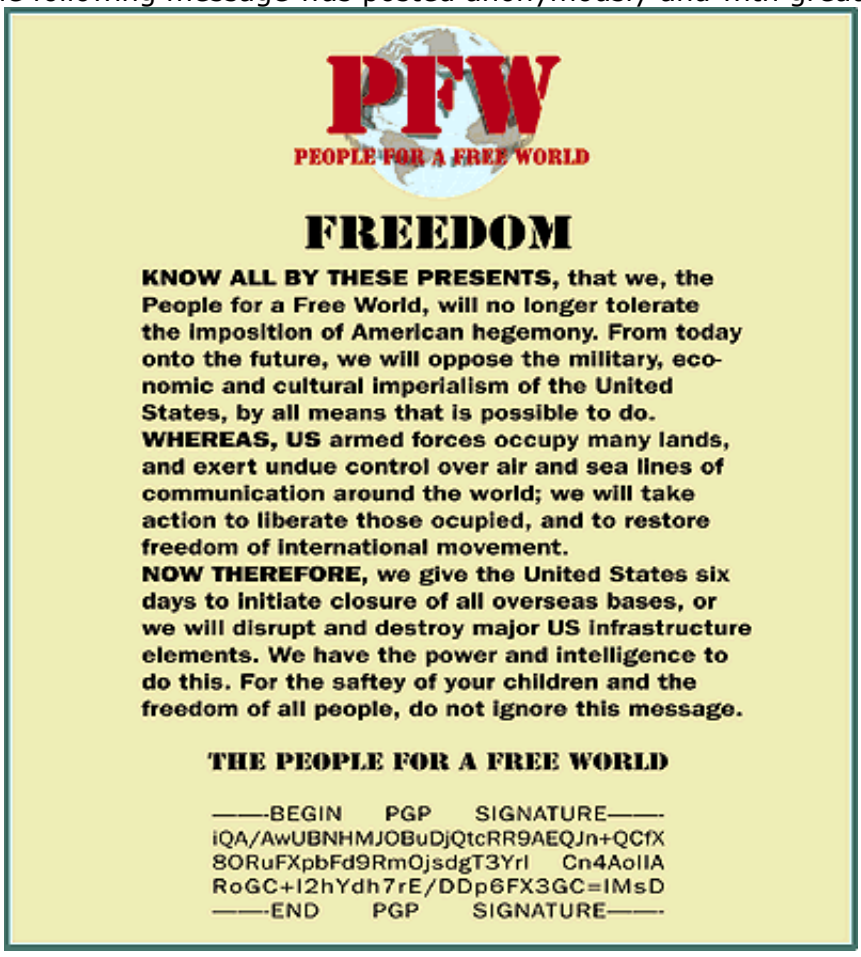
The Great Cyberwar of 2002

In this Wired scenario, Liddy Dole faces the biggest crisis of her presidency: the first global cyberwar, where the enemy is invisible, the battles virtual, and the casualties all too real.

By John Arquilla

10 July 2002, 12:04 PDT

This time it is real. The great cyberwar has begun. I am sure of it. I have decided to record whatever happens here because I am certain that one of the many scenarios I have studied over the past decade is now taking place. Two days ago the following message was posted anonymously and with great craftiness on several commercial news sites:


PFW

PEOPLE FOR A FREE WORLD

FREEDOM

KNOW ALL BY THESE PRESENTS, that we, the People for a Free World, will no longer tolerate the imposition of American hegemony. From today onto the future, we will oppose the military, economic and cultural imperialism of the United States, by all means that is possible to do.
WHEREAS, US armed forces occupy many lands, and exert undue control over air and sea lines of communication around the world; we will take action to liberate those ocupied, and to restore freedom of international movement.
NOW THEREFORE, we give the United States six days to initiate closure of all overseas bases, or we will disrupt and destroy major US infrastructure elements. We have the power and intelligence to do this. For the saftey of your children and the freedom of all people, do not ignore this message.

THE PEOPLE FOR A FREE WORLD

-----BEGIN PGP SIGNATURE-----
iQA/AwUBNHMJOBuDjQtcRR9AEQJn+QCfX
8ORuFXpbFd9RmOjsdgT3Yrl Cn4AoIIA
RoGC+I2hYdh7rE/DDp6FX3GC=IMsD
-----END PGP SIGNATURE-----

This declaration appeared on the front page of the CNN site at 8:30 on Monday morning. The CNN chief webmaster issued a statement an hour later claiming that it was not an official post and that their logs showed that no one inside the company could have posted it. Within seconds of appearing on the CNN site it also appeared on other high-traffic sites, such as USA Today, The Guardian, ESPN SportsZone, Disney.com, and Africa Online.

It seems like a great hack, and it is. But from the moment I read the declaration and saw the few headers from it that were posted, I felt deep in my being that this was no joke.

All day Monday the cyberpundits deconstructed the hack. No one is taking it seriously. The old gurus of online security have focused on the technical aspects of such a widespread, simultaneous, and up-front hack. The webmasters have been embarrassed and admit they have no idea how such a broad prank could have been pulled. How can you post a notice on a front page without anyone official noticing it? It even made it onto the evening news and the morning papers.

But by Tuesday it was off the TV news. I began looking at what logs and data I could find - most of it posted on the instant site www.peoplefree.net/ that got going yesterday - and the more I read the more worried I became. I'm worried about the nondescript and inconsistent origins of the headers, worried about what the declaration said.

Then this morning at 10:30, the president issued a press release, which I read on MSNBC. And this is what has me worried the most. She said that the message "superimposed" on CNN and on other news Web sites is believed to be a hoax, and that it is typical hacker mischief to be deplored, and not to worry, blah, blah, blah. It's all under control. She also said "our country has the best infrastructure monitoring system and is ready to protect critical systems throughout the country should there ever be an emergency."

That worries me because I know what this means - it means they'll activate that still-born, Clinton-era disaster, the Minimum Essential Information Infrastructure (MEII). Hah! It's a load of horseshit. It couldn't protect a welded storage container. And I've told them that more than a hundred times, which is why I was dismissed.

So yesterday I got two of my top Naval Postgraduate School students here in Monterey to help me process whatever we could find on the case. We decided to consider ourselves a crack cyberwar deterrent team. Ivar and Connie think it's all very educational. I think it may be the start of something very ugly.

But we have no cred to do this. It doesn't help when you have to call from the Naval Postgrad School and ask someone for a sensitive path routing. "The Naval what?" they ask. "Are you calling from a boat?"

Connie has been terrific. She has turned down her Living Death CDs and amassed quite a mountain of data in the last 24 hours. Ivars has contacted the owners of as many of the hacked Web sites as he can to obtain logfiles and just anydamnthing else he can wrangle away from them. He's also discovered several newsgroups where the declaration was posted that were not mentioned before. As we expected, the "People" used several anonymous remailers to brush over their trails on Usenet, but Ivars noticed that the sequence of remailers was unusual.

11 July, 10:07 PDT

This morning Connie scammed a chunk of time on the campus Cray. Peterson's uploading the latest rev of the language analyzer. I owe him a six-pack of Budweiser. Ivars came in this morning, after staying up all night; he says the route analysis points to two sources - not a single source, but not a dozen sources either. None of the tracking sites have mentioned this.

The news agencies are giving the PFW declaration less coverage than the fucking weather. Heat wave in

the West - now there's news.

Ivars noticed that the deadline date from the People is Bastille Day. I think this is ominous.

I've spent the morning discreetly calling around my former contacts (the ones who will still talk to me anyway) at Foggy Bottom and the Company. They really don't seem to know anything. Then M. just sent me this background paper summary that is being passed around. To my eyes it all lines up to some serious potential trouble:

> Recent Conditions of Instability 1. At urging from the United States, NATO's next round of alliance expansion in May to include Lithuania, Slovakia, and Romania. Despite Lebed's sharp objections, the alliance leadership unanimously resolved to bring these benighted countries into its protective embrace before the end of the year. 2. Taiwan's formal declaration of independence, also in May. China vowed to recover the island "by all necessary means." The United States provided no direct security guaranty but did warn China that it should pursue "only peaceful means of conflict resolution." 3. Days later, Russia and China entering into a cooperative entente to enhance their mutual security. Their deal: China will invest in the industrial modernization of Russia in exchange for military hardware. (This has the Pentagon alternately gleeful, because it could mean a new arms race, and unnerved, because it could empower the Russian communists, and they're already making a major comeback.) 4. North Korea found to be pursuing a nuclear program in violation of Carter's 1994 disarmament agreement. The US immediately suspended grain shipments, reimposed tight economic sanctions on Pyongyang, and sent an additional carrier battlegroup to the Sea of Japan. 5. Iran and Iraq exceeding the tentative peace treaty reached in 1990 and entering into a full-defense corporate pact. (Ditto Pentagon reaction in No. 3, different global theater specialists.)

We need to rent some electrical generators quickly.

12 July, 08:11 PDT

Late last night before going to bed I read the first posts that even mention the possibility of war. But they were posted in alt.conspiracy.

Went to the hardware store this morning. Grabbed a Honda generator, and a dozen jerry cans. Ivars is getting them filled with gas now. Also batteries, some garbage containers for water, and the usual emergency food supplies in bulk at Costco. I got not only a pocket transistor radio, but also a ham radio and a solar-powered spectrum scanner. Also got some packet radio stuff to send email via wireless. Our room looks like the barracks of some survival nuts. I do feel like a maniac.

I tried to get through to Vreeland on the phone. His secretary had that tone with me. The "General Vreeland warned me about you" tone. I finally did talk to Colonel Pritchett on the phone. He said, "Yes it's worrisome, but if we overreact ... " Overreact! I told him once again about the radar-systems threat, the power-grid threat - but the more I pile on, the more paranoid I sound even in my own ears.

What I see unfolding is "fragment war," waged by a dispersed and highly technical network enemy that strikes with boldness at the heart of our information-based society. We did a whole book on this scenario for Rand in the late 1990s.

Connie is crunching the remailer hops on the campus Cray; meanwhile, Ivars has got the language analyzer working on the message and eight years' worth of Web postings. He's a lateral thinker, so I have some hope.

12 July, 18:00 PDT

Ivars has some results: a non-native English speaker! Connie also came in with some preliminary ideas. She thinks that the two sources, or at least one, is in Asia. Also Ivars thinks at least some of the hacking was done via microwave programming! Supposed to be impossible - and yet they keep trying and maybe somebody succeeded. Data superimposed by transmission through the air ...

Today I fired off the following letter to McKay:

> To: Admiral William McKay, Director of Information Warfare, Pentagon From: Jack Miller, Naval Postgraduate School Dear Bill, The "declaration" should be taken very seriously. Reasons: 1. Language analysis on the text of the message indicates it was written by a non-native English speaker, most likely Korean. 2. The posts to Usenet and logfiles of hacked sites indicate that the data originated from somewhere in Asia. The Minimum Essential Information Infrastructure system is not the answer to this threat. The MEII is largely focused on ensuring the security of presidential command and control functions relative to US armed forces. The system was designed to allow basic military, and essential civil defense, communications to keep functioning after a digital attack. What's called for in this situation is man-in-the-loop monitoring of military and civilian infrastructure systems: finance, transport, power. Possible microwave programming involved, representing another dimensionality to guard. I can be in the War Room this evening, if you need me. - Jack

Things to buy: handheld TV, portapotty? Connie says I'm going bonkers.

But D-day is only 48 hours away. Detonation day. Most important thing tonight is to shield all our electronic equipment. I sent my son out to find copper chicken wire but he could get only the usual zinc-coated kind. I did find lead shielding at the recycling place to put around my computer. I know it's probably nuts. Gonna be lead shielding in my hat next. Maybe I am ... no, not going to say it.

There was only a very tiny mention of the deadline approaching - done with a smirk - on the USA Today site.

13 July, 10:10 PDT

My memo to McKay was dismissed. Politically, McKay can't afford to take me seriously because he is already "extended" for getting me this Postgraduate School position after I was booted from the Pentagon.

We got the iron cage all around the room. And a way to exhaust the shielded generators, too. Ivars tested the setup this afternoon.

We did some more traffic analysis with some "borrowed" spook software comparing all the Web postings on July 8 when the declaration was posted, and when other dissidents were posting elsewhere. The idea is that you can't post more than one thing at a time. Because of the Bastille Day date, we are looking at known French terrorist groups. This process of elimination hasn't yielded a result yet because it's taking hours to compute, even on the Cray.

I went back to our Rand study on infowar. Even the Dole administration's denial is according to the script!

Tomorrow is the People's deadline. The only thing I can do now is wait for them to strike. Seriously, God: it's OK if I'm wrong this time.

14 July, 09:44 PDT

Power outage! Hey it could be from something else. At 9:20, I was watching CNN, MSNBC, and Fox News when my three AC-powered televisions went dark. The DirecTV programming on my battery-powered set showed static for several seconds, until the stations' generators kicked in. (We fired up ours soon after.) The news says the outage extends down to Los Angeles.

Phone lines are dead too. McKay couldn't reach me if he wanted to. (Hunch: now he does.)

Twenty minutes into the blackout and the office is already becoming uncomfortably warm. It's the heat wave combined with all this gear and the generators, sans air conditioning - I hadn't thought of that problem.

14 July, 13:54 PDT

The latest TV news reports indicate that three 500-kilovolt transmission lines extending from hydroelectric dams along the West Coast were knocked out, interrupting electricity and phone service throughout California and Oregon. The executive director of the Western Systems Coordinating Council reported that the problem has cascaded throughout the grid, knocking power plants offline in Rock Springs, Wyoming, in Hells Canyon, Idaho, and in Brush, Colorado, causing outages in several western US states.

Reports by noon or so also indicate that no signs of sabotage have been detected. That means no physical destruction of the system.

Electrical engineers posting on professional sites reported that the PFW uncovered several coded pathways into automated controls that govern the power grid; not one, several. Unsurprisingly, the codes and firewall gate locks were way outdated. So: microwave programming was not necessary (that was paranoia - I shouldn't have let Ivars talk me into that one; makes me look ... worse than usual). They used standard - but beautifully tooled - techniques.

The declaration-blackout connection is the only topic of discussion on TV now. Pigeonlike flocks of pseudo-experts cooing reassurance: it's not terrorists, dear children.

The generators are up here but the phones are still down. The Web's blacked out to me too. I hear via direct broadcast TV that sources on the Web claim this is "just the beginning" - nuclear power plant meltdowns in the offing. Our scenarios said they couldn't do that because they are not on the same sort of grid entry. But ... would an outfit claiming to be struggling for the people kill millions of the people? Concern for bystanders never stopped this type before.

14 July, 18:00 PDT

Zap! That's what the logo for the evening news says. The event is being named the Big Zap. I hear there are already "zap sites" up, tracking the event. Those parts of the Web still running are reporting record traffic; some zap sites are getting millions of hits per hour. The UFO sites are apparently also overflowing with reports that it was not terrorists who deadened the power grid. Be funny if it weren't sad. The Union of UFO Realists - a surprisingly large voting bloc - has demanded to see the president.

The wireless email gear never worked because the outage was too widespread. Only thing reliable now is AM radio and DirecTV. Ham radio is wonderful, but exhausting.

15 July, 06:15 PDT

Power and phones came on last night around midnight.

Half an hour later they were switched off again - like, mockery! In the half hour they were up I got a decent dump of emails. Among them were several notices that the severity of the outage requires a complete clean bootup that in some cases was taking longer than the actual outage.

Reported fallout: 35 known deaths so far, from traffic accidents to heart attacks. Lots of heatstroke victims among the elderly. The zap sites report that economic damage has hit the billion-dollar mark. Rumor has it that in a part of California still unpowered a dam broke, killing thousands. Assuming the last is only a rumor, the total effect is mostly inconvenience. It could have been a lot worse. A lot.

Several folks in the unaffected parts of the country passed along a notice from the People that appeared on the Web: "Perhaps the president's next statement will not be so smug and assured." This also had the same crypto signature.

The president made a statement again. The protective measure she announced three days ago - the MEII - is focused, she said, on ensuring the security of her command and the control functions relative to US armed forces. That's great, but, as I keep saying, it won't do a damn thing when it comes to shutting down everything else.

The MEII just sent this spam to all US netizens: "Please use email sparingly until all parts of the country have power and communications service. Email clogging is hindering the efforts of emergency agencies."

15 July, 09:31 PDT

The PFW posted another statement (again, on a number of Web sites, all different from the ones they used to post their declaration). They promise more attacks unless the US government accedes to their demands.

I called a friend at the FBI and learned the Feds admit (in-house) that yesterday's blackout was the work of hackers and that the second message is likely not another hoax. The attack was hardly nuanced - the attackers had engaged in a brute-force search for login passwords. (Friend is emailing the log-attempt records.) But backtracking to the source, the Feds found an indication only of uplinking in the Pacific: signal indicating size of equipment. A small ship at sea, quite possibly only a few hundred miles off San Francisco! So it did come through the air, in a sense. May have used one of the NSA's own satellites: piggybacking the carrier wave. Which means they have access to all the NSA data?! No, they'd have to have the code too. All that still murky.

Power has been back on for six hours. The phones are just now back on for the past hour. I've been trying to get on the Web, but it is almost at a standstill with traffic.

15 July, 10:45 PDT

Waded into the Web finally. I learned from the New York Times-sponsored zap site that the government's Cyberspace Emergency Response Team did a credible job of damage limitation (taking into account how mediocrity rules) - but was constrained by the architecture of the power grid, which was hardwired for automatic sharing of slack resources - a weak point exploited by the attackers.

Connie is running the analyzer on the new post and on the login records.

15 July, 15:27 PDT

The AP zap site has posted an interview with an unnamed hacker who claims to have been "exploring" in the power grid during the time of the attack. Claims he detected the detonation of a powerful logic bomb that forced the system controls to repeat their emergency energy sharing procedures endlessly. He claims he attempted to override the system controls when he saw what was happening, though he failed to stop the catastrophe. It's just websay - except it fits in with what we know.

It's not over. In fact, I think it's only just begun. Ivars went to San Jose to collect some backup tapes of the Net so he can do some more crunching. Connie wants to stay the night and monitor the traffic data. But, I think she's scared. We all are a bit jittery.

17 July, 09:16 PDT

Second attack has come. Body count: 463. Cause: midair collision. The air traffic control system was cybotaged. News reports indicate that FAA personnel complained that their radar screens were freezing, and were switching data tags (such as aircraft altitude data) between close-flying planes. Series of near-misses in skies throughout the country - and one head-on collision between passenger jets in a thunderstorm over Michigan, resulting in the deaths of all aboard. It's suspected that the automated route and altitude management program's collision-avoidance algorithm was damaged. No reports yet on how they got in. A couple of zap sites have posted theories, some of them pretty good.

An hour ago the US grounded all commercial flights; few exceptions. Military flights continued, with Norad and the Defense Information Systems Agency's "continuity of operations" center in Slidell, Louisiana, placed on round-the-clock alert - despite the complete absence of any hostile air activity. They're alerted for the wrong thing, dammit! Suppose military air systems are hacked into and some of those planes are carrying live ordnance. Maybe air-to-surface missiles? Meanwhile, economic losses from the groundings will amount to billions daily.

On the Net, the outcry for revenge against the PFW grows thunderous - but it is almost shouted down by the vocal minority coming out of the cybernetic woodwork: "We're getting what we deserve!"

The little girl who died when the power went off in the hospital during her operation is getting major ink and airtime.

A message posted to 50,000 newsgroups from a group known as The Dove of Jihad claimed credit for the attack. As they're an obscure Sunni sect known for abjuring the use of any technology, their claim, made during prayers in a mosque in Aleppo, was disregarded. Other Islamic splinter groups also claimed credit, along with a white supremacist faction and an Andorran anarchist syndicate. These claims were swiftly dismissed, too: all were missing the digital signature the PFW had in both previous site hacks. The most outrageous theory as to the identity of the People came on a zap site called the Zap Theorist. It says the whole thing is a Hollywood plot to generate movies after a very slow two years. The fact that one of the very first postings of the declaration was on The Hollywood Reporter site - even before it was on the TV network sites - is what gets its supporters excited. Ivars noticed this earlier, but we didn't know what to make of it.

17 July, 16:41 PDT

I sent another memo to McKay earlier today, with the results of our latest analysis. The power grid blackout was caused remotely, and the attackers left a footprint similar to the one belonging to whoever posted the PFW's messages to the Web. Connie made a brilliant suggestion. She says that the PFW probably encoded the logic bombs with their crypto signatures - as a way of proving they come from them. She is betting they are there, and is trying to squeeze the logs from the FBI.

Received a call from McKay's secretary to proceed immediately to Moffett Federal Airfield in Silicon Valley to take a military air transport to Washington. He's bringing me back from "internal exile" to act as his staff aide. I'll participate in the president's Executive Committee meetings. Back in the Pentagon as if my history with them never happened. About face!

Latest theory of the day, courtesy of one of the zap sites: The Islamic Salvation Front in Algeria is trying to implicate France (explaining the Bastille Day date of the Big Zap) in the attacks as a means of distracting Paris from its support of the embattled Zeroual régime in Algiers.

18 July, 11:04 EDT

Pentagon. Full-scale defensive Big Zap 2 alerts continue - but, again, they're unduly focused on "critical" or "minimum essential" elements, because that was the strategic approach taken during the nuclear era.

At the ExComm meeting today I pointed out that when the October 1997 president's Commission on Critical Infrastructure Protection issued its report on cyberterrorism, the avoidance of the strong-encryption issue - and the insistence that the government have access to corporate encryption keys - led to extreme American vulnerabilities.

A key person in the new group is a former colleague and someone whom I greatly respect: Bob Stevenson. He and I have been up since four o'clock this morning, cobbling together an estimate on developing point defenses of vulnerable nodes in finance, power, and transportation systems. The answer: several weeks. Now McKay says "not good enough."

Meanwhile, the PFW called a 72-hour "pause" - to give the US government time to reflect. The president remained obdurate. A USA Today graph indicates that, instead of public opinion "rallying around the flag," as expected, the president's baseline approval rating is being battered. She has dropped from the mid-80s down to the low 60s in four days.

There is a growing online faction that - predictably - believes the PFW is a government sham, a psy-ops scheme designed to allow the United States to declare martial law and create a police state so that the prez can become a dictator - the usual horseshit.

The Net remains a hotbed of activity. Zap sites are full of accounts by "good guy" hacker warriors trying to gain electronic access to the attacked sites to develop information for their private investigations. The main thing they are doing is adding to the confusion. But then to a lot of these "good guys" chaos is a good thing. The president promised all "vigilante hackers" would be nailed for obstruction of justice. She also reaffirmed that the United States would not bow down to the PFW's threats. But "hacker militias" are gaining popularity anyway.

21 July, 01:15 EDT

The lull in the attacks gives us time to anticipate likely targets. Electric power on full alert, in case of a return Zap attack; and oil and natural gas SCADA (supervisory control and data acquisition) systems were also alerted. Commercial flights continued to be grounded, so the air traffic control system was simply monitored for intrusion - to guard against the emplacement of "sleeper" mines and dormant viruses that could later be activated.

The financial sectors were on perhaps the highest state of alert of all the dimensions of the infosphere - markets were very jittery. Some of the more high-flying speculative businesses are going belly-up in the chaos.

New faux industries sprouting up overnight. I got this spam this morning: "Is your bank secure from terrorists? Don't count on it - banks are next! We evaluate your bank's break-in potential! Talk to us!" Then you give them enough info to break in themselves. Nice scam.

There was a report today about how Shell Oil had to sheepishly admit that in its panic it hired some con artists pretending they have the know-how to stop the PFW from breaking in to its system. These kids (they were only 12) couldn't install a videogame.

21 July, 08:45 EDT

Hot newsmail: a computer-controlled chemicals factory just blew up in Detroit. Took most of eastern Detroit with it. Trying to search for more info. None yet.

My sister lives in Detroit. Can't get through, lines jammed. June called, asked me if Laurie's OK. Can't find out. "I told you so" is cold comfort.

21 July, 18:18 PDT

Back in Monterey now. I feel less impotent in the lab. We've been working on leads given by the location signature sensors, which linked satellite and ground station data in an effort to triangulate on the physical point of origin of particular attacks. These efforts were only partially successful, as the LSS system could work only when the PFW used international phone lines or radio uplinks - and functioned much faster in the latter case.

LSS analysis suggested that one attack was launched from a site in Colombia, another from somewhere off the east coast of China; then we have our own boat-off-California theory. A floating command center, always on the move: impossible to locate unless we get lucky.

But it looks like we've now got new programs online to protect the majority of our power grids ... including jury-rigged shielding against microwaves and EMPs.

Haven't heard from Laurie yet. Worried.

22 July, 09:09 PDT

Waiting for a looong analysis to finish crunching the latest triangulation. Nothing to do but log - as if it's doing something ... The Washington Post has a story about the Committee of Information Scientists claiming to have evidence China is behind the attacks. Agreed to share their data (drawn from their own Internet monitoring system) with the government. First we've heard about it. There's a call in to them now.

It's always been there, in the back of my head. Cyberwar. It's now in more and more people's minds. I can see it here at the school. Connie was white-knuckled on the keyboard and kept making typos as she sent queries about this; Ivars called on the videophone - this facility has one - and he was having some kind of panic attack. Younger, not as good at hiding fears: Could this lead to World War III?

China denies everything. Prime Minister what's-his-name says, "This is not the People's War." Just how panicky are Americans going to get, accusing China - a nuclear power - of being behind the attacks? Cyberwar. No longer just the Big Zap. Online magazines have pretty digital images of computer screens with mushroom clouds on them ...

22 July, 15:53 PDT

New zap. The Trans-Alaska pipeline has burst near Valdez. Damage reports are sketchy, but a helicopter view of the scene looks bad. Are we assuming it's cyberwar when it's just coincidence? No such luck - computer-controlled leak alert systems seem to've been virused.

Zap sites, especially Zap!, are getting this news before I hear about it on my government e-clips. I'm not sure what to make of this: incompetent government intelligence, or are the zap sites themselves somehow involved in the crisis? That is the theory of the antizap sites.

22 July, 17:35 PDT

The strangest news tonight. Two pimply college students shot dead in their garage this morning by vigilantes because they were pseudonymously taking credit for being PFW. Hysteria killed two kids - which brings me to Ivars.

It's scary. Ivars tried to get in to see me this afternoon - and was arrested. Seems his eye scan turned up a conviction for illegal hacking six years ago, age 18. Hid it from the Navy but not from internal affairs. So two young IA guys, faces like babies, come into the lab to question me. I get the feeling they think I might be with the PFW because of my association with Ivars. Suggesting maybe I was bitter about being tossed

out of the Pentagon and am trying to prove I'm right. Witch-hunt time.

I at least got them to call McKay, and he called them off. And got Ivars released, but Ivars is probably under surveillance - and probably so am I. Connie says she's being followed ... nowadays I can't say "Maybe she's just being paranoid."

Stevenson claims that - thanks to the heightened monitoring system we've set up - he's already got a bead on the attackers. Maybe I'm not tits on a boar after all.

Still no word about Laurie. Want to go to the area, look for myself. Phone lines go up and down, up and down - if she's alive she's probably trying to call.

Decided to move to DC for the duration. Packing tonight.

23 July, 10:08 EDT

The primary environmental damage of the spill has been estimated to fall in the US$1 to $2 billion range. It's like wounding a man and then pissing on him.

The attackers used what appears to have been a polymorphic engine to insert a virus into the SCADA system that regulates oil flows in the pipeline. The virus attacked and disabled the leak alert systems (which monitor pressure and flow rate deviation) making it impossible to detect the increased oil pressure resulting from a series of remotely directed commands to increase flow rates at several pump stations simultaneously. When a scraper pig (a robotic device that cleans the inside of the pipe with a polyurethane cone) was lodged in front of a check valve, the valve burst.

The good news is that our team has pinpointed two attacker sites: one in an area of Colombia under control of the Cali cartel, the other on one of the smaller Spratly Islands off the coast of China, consisting mostly of a reef and some built-up structures on stilts. Bad news: the sons of bitches are probably highly mobile. But if we move quicker'n they do ...

McKay told me that two companies of Army Rangers will lead the way to the Colombian site, while a Marine assault unit will undertake the operation in the Spratlys.

New USA Today graph: The president's approval rating is lower than morale on an icebreaker out of fuel. Small wonder then that she ordered the raids just minutes after getting the ExComm's recommended plan of action. Meanwhile calls for blockading Chinese ports. One step closer to war.

24 July, 21:42 EDT

What a day! Here's what happened, though most of this will not make the news tonight, if ever. Operations Triphammer and Javelin - Colombia and the Spratlys - launched earlier today, half a world apart, but nearly simultaneously.

A debriefing memo I got to see quickly reports both of the US strike forces were large "packages," requiring a lot of transport and combat support - all of which made them easy to spot as they moved to attack. Indeed it seems as though one of the raids had been fully expected. The Triphammer force found an abandoned base of operations - only after it fought through a teleoperated machine gun and mortar defensive system. (Nicely conceived - and bankrolled. Who's paying for all this?) When the Rangers reached the control center, the facility itself was remotely exploded, killing scores of them. Colombian government protested the incursion. Senator Trumball said, "You know what? The Colombian cocaine-money government can kiss my rebel ass." And most of the country approved the remark - one that would've been condemned a year ago.

As the second raiding group was on its final approach to the Spratly site, the Marine amphibious landing ship carrying the strike team was struck by a remote-controlled rising mine that detonated under its keel,

breaking the ship's back. Javelin proceeded anyway, with three helicopters full of Marines lifting off the crippled assault ship and storming the reef. This time, they found an occupied, operating control center, and had apparently caught the enemy completely by surprise. After a brief but vicious firefight, killing 20 defenders at the site, the Marines captured four prisoners and a few pieces of equipment that were not destroyed in the fighting. Hoping these guys aren't decoys.

Where's Laurie?

25 July, 15:39 EDT

The president spoke to the nation once again, this time mourning the loss of so many Rangers and Marines; but she also noted the great payoffs these raids would have in the coming days. As she put it:

"Once again, America is being protected by its brave rifles. And, God willing, they will continue to press our cause on to victory. For our enemies fight only from the evil shadows. They must lose this war in the end, and will disappear - forgotten - from the face of the Earth ..."

No amount of eloquence could change the fact that the president's approval rating is now at 12 percent. She's worse off than Nixon at the height of Watergate. One good thing: apparently the raids found nothing implicating the Chinese.

The most dramatic event of the day, though, was the delivery of a tape in Kabul that was passed by a nameless street kid to CNN's Christiane Amanpour as she was reporting from the field in Afghanistan. It was a recorded message from "Talus," a self-described spokesperson for the PFW. Amanpour played it over the air for International Hour. While Talus rambled a bit, he made himself clear:

"The PFW are diminished by the loss of their heroes, but their blood can only consecrate our purpose. A final offensive will be launched as soon as our forces, which are as numerous as the grains of sand in the desert, can gather for the final blow."

It all seems authentic. The CIA's memo to the ExComm claims the tape was made in Kabul that day, from another tape that was played over a cellular phone. Kabul! At least now we know who the bankrollers are ...

Analysis of Talus's sonorous voice showed that it was computer-generated using a popular freeware program.

Zap! reports that hacker sources have confirmed "beyond doubt" that there was some sort of Russian involvement in the PFW. Hacker sources are rarely "beyond doubt," that's my view. That's where Connie and I disagreed. The specific claim was that the Russians were using the Cali cartel as a third-party proxy to give them some "plausible deniability." The NYT reports the official line from the US government: evidence linking Russia to the cyberwar is only circumstantial and has to be weighed against repeated Russian denials of guilt and offers of assistance in pursuing the PFW. But we just might be back on the World War III track again, dammit.

Also on Zap!: the Online Nation has claimed that the PFW is an attempt by government intelligence agencies to discredit them. For the past two years, the Online Nation has been pushing for recognition of its status as a "nation in cyberspace." Said status includes freedom from paying US income tax because "our lives are lived predominantly online." It is true that online lifers are getting no respect these days. The word online is enough to put some folks into a choking rage.

27 July, 07:36 EDT

Our data-crunching efforts offer abundant evidence that Russia and China were involved in, if not behind, the attacks, and were using both the Cali cartel and the Asian triads criminal organizations as cutouts and proxies. Yes - China after all! Now they're back in the picture! The information developed from the Spratly

prisoners, all Malaysians of Chinese descent, matches our data analysis.

The rumor around here is that the Spratly prisoners had been subjected to the most advanced interrogation techniques. Nice way to say they fried their brains with drugs and who knows what. Statements they made at least confirmed they were fighting for the cause of the Sino-Russian consortium. General Vreeland suggested the unspeakable: a nuclear strike against a single selected Soviet outpost as a warning - they'll back down after that, they haven't got the nukes anymore to return fire effectively, he claims. McKay and I stared at him in horror - were even more horrified at how the others took the suggestion seriously. Nodding silently. Luckily the president only sighed in disgust and said, "You look for powder kegs to throw your cigarettes into, Vreeland?"

"Look, let's give 'em a kick in the ass for a slap in the face," McKay said. "But we do it with Jack's methods."

Everyone looked at me. The NSA director with narrowed eyes. I was still under suspicion and only the president's insistence kept me in the loop. "We could retaliate cyberwar for cyberwar ..." I said.

The president said, "Maybe. But that could be almost as provocative as a nuke."

She started to talk about sanctions and I groaned inwardly. But McKay and I resolved to work up a cyberwar contingency plan and the secs of state and defense encouraged us.

27 July, 11:17 EDT

Email just in: the president assented to the ExComm's plan, despite Russia and China's continued denial of any involvement in the attacks on the United States. Sanctions, plan for our own cyberwar. Meanwhile Americans are logging on to communicate with Russian and Chinese netizens by email and with ordinary citizens by fax, urging them to protest their governments' secret "cool war" (an allusion to Frederik Pohl's famous story about clandestine future warfare) against the United States. We'll see if the Internet lives up to its hype.

It was amazing to me to see how much the military was relying on the zap sites for intelligence. As I noted earlier, they often have the best information soonest. Usually military intelligence would only confirm a fact. It had 25 full-time surfers reading all the sites.

I was in the hall on my way to the computer room when I overheard the sec of state (a member of the ExComm) shouting at a red-faced undersec that the idea of private citizens trying to bring an end to the war could only "escalate an already serious crisis that needed only a slight nudge to trip over the nuclear precipice." I ached to tell her she was full of shit, but it doesn't matter: she and the government have no real control over the Net and that's the Net's strength.

27 July, 13:45 EDT

The US military is feverishly preparing for its retaliatory campaign, Operation Cyberlord (the infowar aspects of which are called Digital Storm). The plan has overt and deniable elements. Openly, it relies on Special Forces quick-reaction teamsof 8 to 10 soldiers to strike at and physically destroy detected attacker nodes located anywhere outside of China and Russia. Vreeland wanted to go for select targets inside their borders with surgical nonnukes. But cooler heads? Well, they didn't prevail - they sent it to a study committee. Same thing.

One of my jobs for McKay was to defend the use of such small teams to the ExComm. I argued that less is more. Smaller the units were, the more teams we could field.

Based on data gleaned from the previous attacks, from zap sites, and from the Spratly raid, US intelligence is able to confirm and physically locate 13 operation centers in the PFW's attack network. All

are outside of Russia and China, most being in ambiguous or disputed territory, just like the Spratly site. All are to be hit in the opening hours of the counteroffensive.

The president finally authorized retaliatory information warfare attacks. These attacks are to be made deniably, keeping this part of the war "cool," but it was hoped that Digital Storm would be unleashed with such fury - and effect - that the PFW would soon feel compelled to call a halt to the cyberwar.

Unlike the deliberate pace of the PFW's attacks on the US, the American approach to cyberwar would be fast-paced and wide-ranging - the kind of all-out approach that historian Russell Weigley once described as "the American way of war."

1 August was set as the starting date for the counteroffensive.

01 August, 16:50 EDT

We all have doubts about a counterattack. It could lead to a nuclear exchange. You get a country frustrated with cyberwar, and if they think they're going to fall apart anyway, maybe some hawk takes over, then maybe he hits the launch button. But of course we can't just sit here and let them bleed us to death - death of a thousand cuts. A railroad here, a city there, maybe a couple of passenger jets, until our whole economy collapses and ... and, just maybe, we end up with the destabilization, the hawk in charge. Military coup, American style.

The doubts are too late. We're committed.

Finally heard from my sister Laurie. She's OK! Some kind of hellish evacuation scenario in Detroit, I guess - riots, military transport buses having to smash through a roadblock of looters run by the Detroit Crips. It's strange we had not heard about this. But there is so much else in the news these days.

Operation Cyberlord commenced this morning with US Special Forces troops on the attack at the same time that covert information attacks brought down, and kept down, the Russian and Chinese power grids.

Pipeline flows in both countries were disrupted, though the Guang Zhou Daily site reports that they were able to avoid an absolute environmental disaster through the heroic actions of a worker who performed a manual shutdown of a whole sector flow - and then drowned in a surge of oil that had already gotten out.

The US attack also extended to cyberstrikes at both the Russian and Chinese financial sectors, wreaking total financial havoc in both. In each case, evolved forms of the Morris Worm were used, to great effect. This particular offensive tool, which features the endless replication and transmittal of nonsensical code, spoiled huge amounts of data on the old Russian Unix mainframes still in use.

Russian and Chinese transportation, financial, and power systems were shut down, causing incalculable economic damage, and preliminary intelligence reports predict that the loss of life was even more severe than that suffered by the US in the opening phase of the conflict.

I keep telling myself: they started it, they started it ... I used to be more willing to accept collateral damage.

01 August, 23:31 EDT

Cyberspace-based attacks on the United States have resumed, aimed at the financial sector. However, as The Wall Street Journal reports, this is the best defended area of the American infosphere. Each attacking node is quickly targeted by Special Forces and interdicted.

02 August, 09:01 EDT

I was in the Pentagon cafeteria, eating a sandwich and going over the damage reports of our recent raids,

when the floor under my feet seemed to jump. There were heated explosions in the wiring underneath. At the same time, I heard a tremendous boom. The lights blinked out for a moment before auxiliary power came on.

I thought: It's heated up, gone nuclear.

I ran into the hallway, as did the other diners. Armed soldiers were shouting at everyone to go into the subbasement through the stairwell. I ran into my office to grab my laptop and followed the crowd downstairs. There were no secondary blasts. Rumor spread that it wasn't nuclear. It was a kind of EMP bomb. Think huge microwave blast - on full power. It's total chaos outside. People burned. People with half-cooked brains, jabbering. Cars stopped in the street - their electronics fried - blocking ambulances and police. I can't bear to even talk about it.

02 August, 09:46 EDT

My laptop has stopped working - the least of my worries at this point - and I am writing on a pad of paper today. I'll enter this into my backup notes when I get a new one.

They had me go to the hospital to get checked out just to be sure. I seem to be all right.

Since no electronics in the whole building are working it took a while to learn that a megapower microwave bomb was detonated near the Pentagon's riverside entrance. Much like a variant on the EMP bomb, it was designed to fry telecommunications equipment, as well as personnel near it. And that it did. This was an apparent attempt to knock out the US Information War Room. But the cyberwar was run from very deep underground and only a few surface communications links were destroyed. The rest of the Pentagon got pretty zapped, though. Were they shielded? Noooooo!

Hardest hit were the people in the parking lot near the entrance. The white coats said that first calculations suggest that this was a far more powerful microwave bomb than any they had seen so far.

02 August, 22:46 EDT

Back in my office, which was relatively undamaged. Phone is acting squirrelly. The president has ordered retaliatory, but still clandestine, attacks on the Russian fleet headquarters in Kaliningrad, and on a Chinese triad communications center in Beihai; apparently the Reds made a deal with their own little mafia.

03 August, 11:05 EDT

There have been no other bomb attacks on US sites. Anywhere. Many in the ExComm take this as tacit evidence that we are indeed fighting a World War III - against China and Russia - and that they haven't the stomach or skill to keep up this kind of fighting. Or other times, I think, China and Russia are planning to take it to another level ... because they know our president is a hesitator. A weak reed, only maybe she isn't and maybe that's the danger. Now I'm thinking like Connie. (And where is Connie? No response to email. Not like her.)

Russia and China continue to deny involvement in the war, pointing accusing fingers at the US and making vague threats about the possibility of nuclear escalation.

The president, whose approval rating has finally started to tick back up, is holding firm, nervily riding out a nuclear brinkmanship crisis. She feels that she is winning the cyberwar, and that nobody will go nuclear first. In an effort to defuse the crisis, the president got on the hotlines with Moscow and Beijing, noting, in seeming sympathy with her Russian and Chinese counterparts, that the United States had nothing to do with these attacks. A friend in the know told me that she told Lebed: "We are all victims." What else could she say?

04 August, 16:18 EDT

Just as the nuclear crisis seems to have passed, and both field and cyberspace operations are running very much our way, the war effort has been struck a grievous blow - from within. Political opposition to the prez's policy.

Today the Committee of Information Scientists fueled the netizen protest movement further by releasing data on Zap! proving that the United States, despite all its public denials, was indeed waging cyberwar against Russia and China.

I must admit that I'm deeply disappointed with this development, as much as I respect the netizens' appetite for the truth. The committee's "outing" of the clandestine cyberwar has had a profoundly unsettling effect in just a few hours. The news is everywhere, and I mean everywhere. The headline on Zap!: Public demands immediate cease-hack!

As the news anchors are fast to point out, the vast majority of Americans don't want any part in a wide-ranging, extremely disruptive secret war at the general public's risk and expense. Polls today make it clear they are strongly opposed to an invisible war in which the effects are felt instantly at home, threatening transportation, financial security, and their very lives. The president's approval rating nosedived.

It will be hard to continue. I have no guess what McKay will do. No press conference today yet.

04 August, 23:51 EDT

Heard from McKay that the president, who had steeled herself to go all the way against the Russians and Chinese, was severely shaken and completely taken aback by the massive electronic protests against the cyberwar. The fact that Americans had outed her covert Operation Cyberlord appalled her. She asked about the protesters, "Do they want open warfare to break out instead? Christ, don't they realize that 'cool war' is the way things are going to be in the information age - and it's better!"

"Hey," McKay snorted. "It's inconvenient. Why ... some people may miss their favorite programs!" Sardonic laughter all around. That sounds like something he thought up to say. But in any case, the writing on the wall is clear: we'll have to shut down Operation Cyberlord very soon.

My fear is that if the CIS and its cronies push us out of cyberwar they could push us into a nuclear exchange! Therefore, if we are ever to obtain proof, beyond doubt, as to the identities of our enemies, we have to move now.

McKay was a Navy admiral, so I argued my case by using the analogy of the codebreakers who helped hunt U-boats during World War II. Sometimes, they held on to intercepted signals, allowing an attack on a convoy to take place - in the hope that the wolf pack would chatter with headquarters just long enough to give them the key to the German Enigma codes. This also meant that they would listen to the convoy's cries for help while the desperate battle unfolded - and not take the steps needed to bring down the aircraft from the escort carriers on the Nazi subs. A dirty business. Which is war as usual.

In one of the riskiest operations of the war, the IW Command temporarily weakened the defenses of the Diablo Canyon nuclear power plant (chosen because we had detected several attempts to infiltrate the plant's control systems in the past several days but had been unable to identify the attacker). We hoped this would give us enough tracking time - before shutting down the attack - to get a full trace.

I'm not going to think about what might happen if we are too slow. That's what Connie was always thinking. Look where it got her. Ivars tells me she was arrested.

05 August, 12:36 EDT

The attack indeed came, a mere two and a half hours after we lowered our defenses. It was aimed at the plant's central system controls by means of a massive logic bomb, or as is commonly known because of its vast disruptive properties, an "I-bomb." We allowed the attacker to hack in, unimpeded.

The nature of the attack suggested that the hacker logged on to the key control systems by means of a brute-force password search, most likely. Then, once online, using the identity of a plant staff member, the hacker was limited only by the usual access controls to which employees are subjected. We let him proceed until a full trace was achieved ...

Delay in taking defensive steps before shutting down the attack allowed partial detonation of the I-bomb - but we did at least avoid the massive cascading effects that would have accompanied a "clean" I-blast. The net result was that the reactor went near-critical, and, because of very strong onshore winds, there was a release of lightly radiated steam over an area populated by nearly 1 million people.

That's all.

Probably most of them won't die from it right away. More childhood leukemia. That's all. That's all. I'll drink to "that's all."

05 August, 18:45 EDT

The ultimate user ID data obtained by the IW Command's deliberate defensive sacrifice at Diablo Canyon gave the ExComm and the president near-certain intelligence that Russia and China were not behind the cyberwar.

While the Cali cartel and the Asian triads were indeed in on the war, the attack center used on the reactor was pinpointed to be in the disputed, territorially ambiguous Abkhaz Republic. From there, electronic traffic analysis showed, most communication since the start of the war had taken place with ... North Korea. The lunatic who runs NK was playing three-card monte with us.

When the president was presented with this information at the ExComm meeting, she told us that the Spratly prisoners, on reinterrogation, admitted that they were intended for capture, and had been instructed to implicate the Russians and the Chinese. How long had NSA and the other intelligence clones known this? Did some of them want conflict with Russia and China - even though they knew, maybe, that it was sourced in N Korea? Should I even be writing this? (They wouldn't let me in to see Connie, who, it turns out, was arrested in DC.)

The overall war plan, according to the leader of the prisoners, was to cause major conflict among the great powers, to allow the triads to take advantage of a long "cool war" to consolidate their control of transpacific trade - both legal and illicit. Yes, North Korea was a willing co-conspirator - but so were a number of other small states - Vietnam, Iraq, Libya - that hated and feared all of the big powers. That is why the cyberwar was designed in the first place - to set them upon each other, in the prisoners' words, "like ravening wolves." Afterward, the world would be safer, as the shadow cast by the great states would diminish, if not disappear - and, maybe, to the victors go the spoils.

Acting on McKay's recommendation, the president called an immediate halt to the cyberattacks on Russia and China. Sent word through diplomatic channels to indirectly apologize. Very, very obliquely ... and deniably, if it came out. At the same time, she ordered a Special Forces assault on the attack center in the Abkhaz Republic. Preparations began immediately, for an attack early tomorrow. She also ordered our forces in Korea to go on war alert.

06 August, 19:22 EDT

Operation Roland commenced, in the breakaway Abkhaz Republic, with a cobbled-together group, including two Seal platoons and one Special Forces A-team.

Kind of thing the public loves: safely overseas, nice and clean. Killing out of sight except through the filters of TV pixels.

The enemy command center was caught by almost complete surprise (finally), and this time - though the defenders were both numerous and well armed - the station was taken, along with much intact equipment. Twelve of our soldiers were killed, but no American programming or blow-dryers or refrigerators or internets were disrupted. So, screw it, that's a success, right?

Initial responses from both Russia and China, while noncommittal, clearly indicated a willingness to de-escalate. Neither wanted nuclear war, and neither could fight a real cyberwar against us for very long. Both made veiled requests regarding the possibility of US aid in rebuilding after the war. The president was, I've heard, tweaked with conscience; she promised aid in rebuilding the Russian and Chinese information infrastructures. All aid, however, was conditional on help in tracking down the transnational criminals and terrorists who had fomented this war - and specific Chinese support in pressuring North Korea to give up its nukes.

07 August, 13:38 EDT

In a midday address to the American people, and the world, the president called for an immediate cease-fire and cease-hack. US forces involved in Operation Cyberlord would stand down. She told the American people that the Great CyberWar had been engineered by several "transnational criminal organizations," in league with some states ("How many, we may never know exactly," she noted). I wonder who ghostwrites this stuff. She added, though, that the PFW was crippled permanently, and that the Great CyberWar would thus have a useful spillover effect - in terms of helping to win the drug war, now that the cartels have been so weakened. She concluded her remarks by observing that Russia, China, and our NATO allies were all "dedicated to ending the menace of cyberwar posed by rogue states, criminals, and terrorists." And all are in support of sanctions against Korea. She didn't mention nuke-radiated steam.

On Zap! (which now has over 12 million visitors a day and has been purchased by Time Warner), the Committee of Information Scientists greeted the president's speech with harsh criticism - and demanded that she own up to having waged an undeclared, secret war against Russia and China. In a news conference the president denied the charge and called for a "time of healing."

At the noon ExComm meeting we learned that the president had authorized launching Operation Cain, a campaign plan for cybotage in North Korea. It was to take place over a period of several months and was designed to cause the collapse of the régime in Pyongyang, leading to the reunification of the peninsula.

31 August, 17:47 PDT

No enemy attacks have been detected for weeks.

The PFW - some real lamers - had very nearly succeeded in duping the great powers into a full-out war in which they might have destroyed each other. And, much as we learned how to shore up our defenses and hone our counterattacks, they must have learned new tactics, too - tactics they will, sooner or later, use on us at a time of maximum advantage and effect.

12 September, 08:26 PDT

Spoke to McKay about Connie and Ivars - said they've already been released! Apparently all the intelligence turned up in the raids failed to implicate them. But ... Connie's family says she and Ivars have "gone underground ... together." I haven't spoken to either of them and so am not sure why they've been radicalized. It could be the necessary hypocrisy. But maybe they had to go underground because they knew they would be followed, monitored constantly. Connie knew too much and had a bad attitude about what she knew. I hope to God she's given the NSA the slip. I don't care which fucking side she's on.

Operation Cain was discovered and defeated - the plan was posted on Zap! about a week ago. Inevitably this incident has complicated efforts to "denuke" North Korea.

12 June 2003, 13:02 PDT

Months later and still none of the combatants in the Great CyberWar have ever admitted their full roles in it. We're all just a bunch of wide-eyed, shoulder-shrugging "It wasn't me, Mom!" kids.

The United States has led the drive, with Russian and Chinese support, for an international ban and convention pledging no first use of cyberweapons. But I wonder how such a pledge can have any meaning.

And of course, any United Nations-ratified ban on infowar will have even less effect on the rogues, terrorists, and criminal networks that fomented the Great CyberWar in the first place. Information Warfare Command is aware of overtures made by leading states seeking the services of these dark cyberwarriors. Everybody wants to hire the toughest asshole on the cell block. Maybe we've got more packs of cigarettes to offer, because our response, to date, has been to start a bidding war for their services ... Business as usual. But not for me.

Been going misanthrope - and I don't really want to be deeply cynical about people. I need a way out. Going to take the lead shields off my computer and off my mind. Today, I sent a memo to McKay, informing him of my decision to return to the Naval Postgraduate School. I ended with a quote from the last oration of Chief Joseph of the Nez Perce: "Hear me, my heart is sick and sad. From where the sun now stands, I will fight no more forever."

END

Date: Sun, 17 Nov 2003 22:05:42 -0500 To: Calvin Tucker From: "Gregg Lanam" Subject: The *real* truth behind the cyberwar?? X-UIDL: 9c1fdfd6ff5abf1beb6e98e1dc4ac845 Hey Calvin, I just found this binary file on alt.cyberwar.conspiracy. It's a clip, anon post by someone who says a friend lifted it from some military guy's files, sucked it right out of his frame. Some kind of new hack called Fish. You need Acrobat to read it, because it has a lot of sound and video portions. And listen I'm not at all mad at you about Sunday night, I was just kidding around. What do you think about this? I mean - if this is really the truth, is anybody surprised that we were lied to yet again?? At least the government is consistent. - Gregg

---

Pentagon adviser and Rand consultant John Arquilla is a professor of information warfare and special operations at the Naval Postgraduate School in Monterey, California. His books include In Athena's Camp: Preparing for Conflict in the Information Age (Rand, 1997).